Platform One

IRON BANK ONBOARDING

Agenda

- Iron Bank Overview
- Container Hardening Process (High Level)
- Iron Bank Onboarding
- GitLab
- Hardening Pipeline
- Q & A

What is Iron Bank?

Repository of Digitally Signed binary container images that have been hardened.

At a high level, a vendor is on-boarded, appropriate access is granted to Gitlab, the vendor makes code, commits to build the docker images, and automated pipelines are instantiated to build and perform security scans on the images.

IRON BANK
DoD Centralized Artifacts Repository (DCAR)

DoD's source for hardened and approved containers. Browse for containers, retrieve scan results, etc.

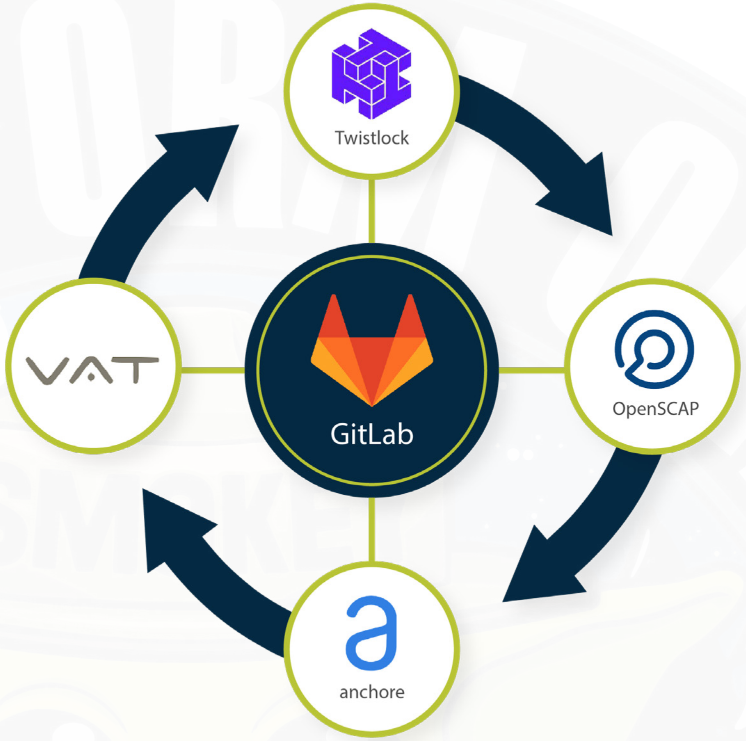
https://ironbank.dso.mil

HARBOR

Browse containers through the official Harbor registry or download via command-line interfaces

https://registry1.dso.mil

Iron Bank Ecosytem



What Iron Bank is NOT

- Iron Bank and Repo1 (Gitlab) are completely open to the public (available at IL2). There are no locked down versions of Iron Bank

- Although the Iron Bank ecosystem contains a functional docker registry, direct uploads of ”external” container images to the registry is not supported. All images pushed to the registry must be hardened and approved.

- The Iron Bank platform does not run containers. Approval of container images does not imply an “automatic” deployment to any specific environment (i.e., Party Bus).

- There are no current built in features supporting license keys, or methods to protect intellectual property (we encourage vendors to incorporate the necessary technologies to fulfil individual licensing and protection requirements).

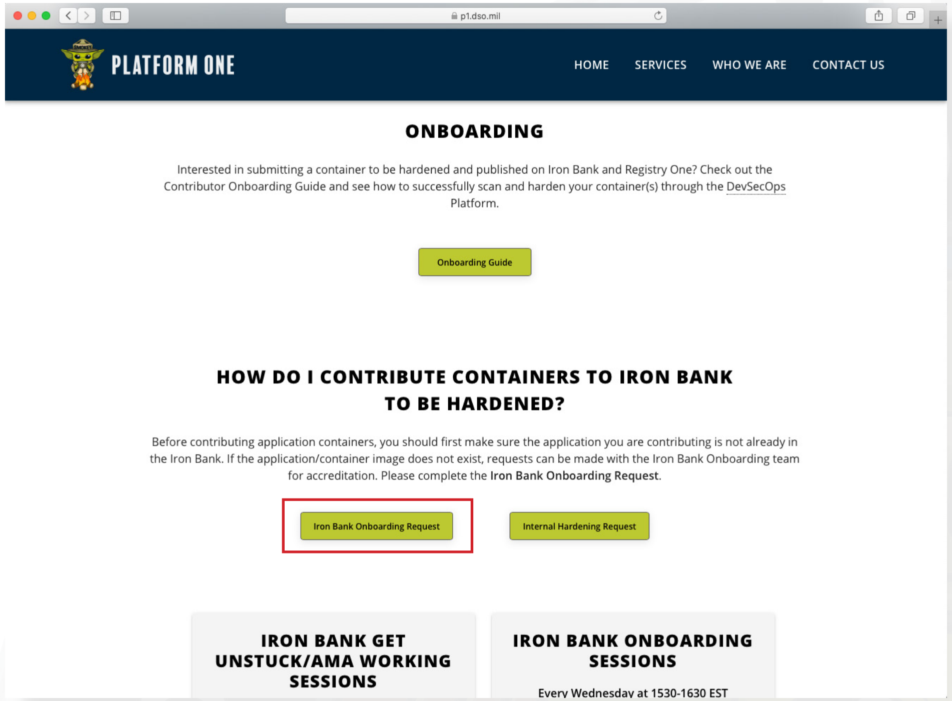
- The Iron Bank is not a completely 100% automated platform. Portions of the “hardening” process are manual and involve substantial human effort.

Onboarding First Steps

Fill out the Vendor/Program Office Onboarding Form

The Container Hardening Team picks up the on-boarding form and creates the organization and repos based on the information provided by the vendor. The next slide shows an overview of the on-boarding process.

Vendors need to register users with Iron Bank SSO system. Register by clicking on the 'Sign in with Iron Bank SSO' button in the sign-in page, followed by the "Register" button.



p1.dso.mil

ONBOARDING

Interested in submitting a container to be hardened and published on Iron Bank and Registry One? Check out the Contributor Onboarding Guide and see how to successfully scan and harden your container(s) through the DevSecOps Platform.

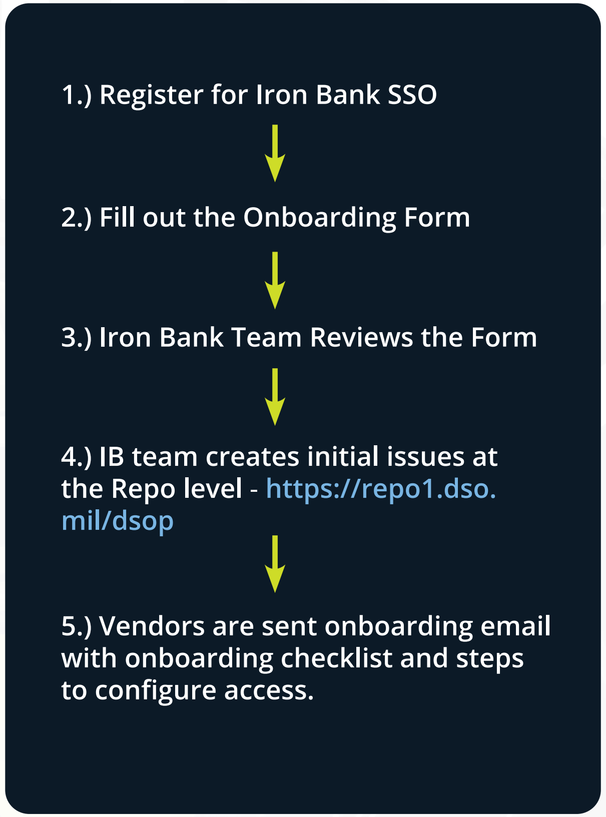
HOW DO I CONTRIBUTE CONTAINERS TO IRON BANK TO BE HARDENED?

Before contributing application containers, you should first make sure the application you are contributing is not already in the Iron Bank. If the application/container image does not exist, requests can be made with the Iron Bank Onboarding team for accreditation. Please complete the **Iron Bank Onboarding Request**.

IRON BANK GET UNSTUCK/AMA WORKING SESSIONS

IRON BANK ONBOARDING SESSIONS

Every Wednesday at 1530-1630 EST



1.) Register for Iron Bank SSO

2.) Fill out the Onboarding Form

3.) Iron Bank Team Reviews the Form

4.) IB team creates initial issues at the Repo level - https://repo1.dso.mil/dsop

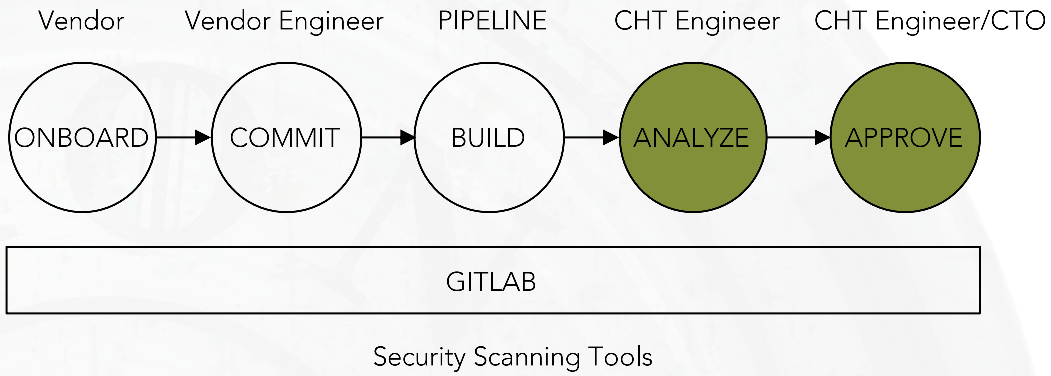
5.) Vendors are sent onboarding email with onboarding checklist and steps to configure access.

High Level Hardening Process

The hardening process is shared between the Vendor and the Container Hardening Team. The following is a description of the process from the vendor and the Container Hardening Team point of view.

Vendor / Iron Bank Development Process

At a high level, a vendor is on-boarded, appropriate access is granted to Gitlab, the vendor makes code commits to build the docker images, and automated pipelines are instantiated to build and perform security scans on the images.

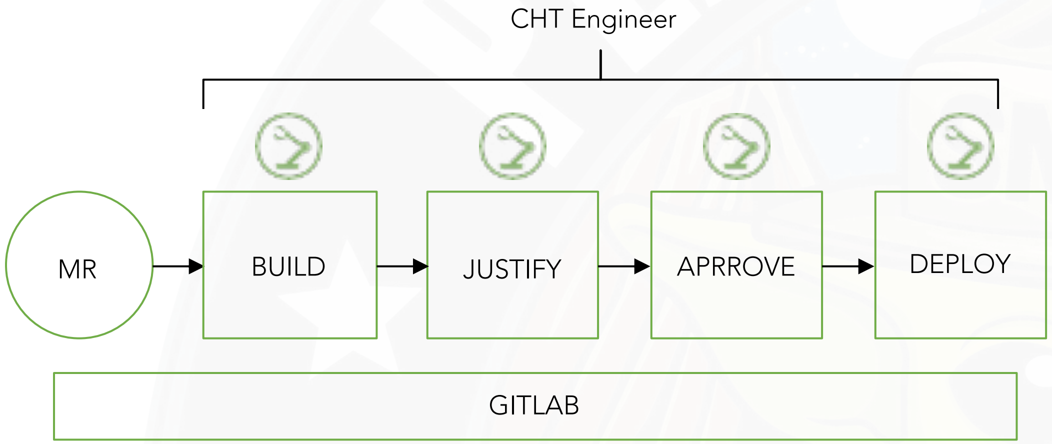


High Level Hardening Process

Container Hardening Team Development Process

CHT engineers enter the process when the vendor has progressed to the point where the pipelines run to completion with no failures. The CHT engineer will begin a justification process where security scanning results are analyzed, minor adjustments are made (if needed) , and finally, the vendor submission is sent for approval.

The CHT high level process is depicted below. Typically, the process is kicked-off via a merge request (MR) initiated by the vendor.



Getting Started

Create a Repo One account to gain access to the public repository of containers.

Start by accessing Repo One at the following link: https://repo1.dso.mil/users/sign_in. You can register by clicking on the 'Sign in with Platform One SSO' button on the sign-in page, followed by the Register button.

1. Submit your onboarding form here. Your repo and issue inside GitLab will be created for you!

Once your repository has been created, an email notification will be sent with a link to the repository, your assigned priority, and registration information for the Onboarding meetings and Get Unstuck/ AMA sessions.

2. Hardening Process

3. Dockerfile Requirements

4. Hardening Manifest

5. Gitlab CI Pipeline

6. Pre-Approval

7. Approval Process

8. Post-Approval

Initial Form Submission

The information in the form allows our team to proceed to create the vendor repos, and associated GitLab issues, however, more information may be needed to improve the overall lifecycle of vendor/hardening processes. Below is a sample of the information the form will capture.

STEP ONE: CONTRIBUTOR DETAILS

Here we will be asking you for basic contact information and if you have a government sponsor or not.

STEP TWO: QUALIFYING QUESTIONS

These questions will help determine if you are a good fit for Platform One Iron Bank. A “no” to any of these questions will pause the onboarding process.

STEP THREE: TECHNICAL QUESTIONS

Technical Questions about your application, these are some of the basic prerequisites you need to have in order to get approved on the Iron Bank. Whether you are a program office or a vendor, these are the technical baselines that need to be adhered to in order to pass the Iron Bank Pipelines. Answering no, will not stop further onboarding, but these will need to be a yes before the containers go up for approval.

Initial Form Submission

STEP FOUR: PARTY BUS OR BIG BANG

Party Bus/Big Bang engagement: Where is this containerized application going next? These answers will help us route you to the next step after Iron Bank and ensure you have a good experience with Platform One.

Sample of KEY questions asked:

- Is your application currently containerized?
- Does it run on Linux containers?
- Can your application build and run in a completely offline/air gapped environment?
- If yes, how many containers are involved?
- List all dependencies of your application requires in order to deploy.
- Is your application currently running in containers on Kubernetes?
- Are your containers accessible from a public registry, private registry, or both?
- Are you okay if your security findings are public?
- Are you okay with your application being publicly available?
- Are there any ITAR restrictions?

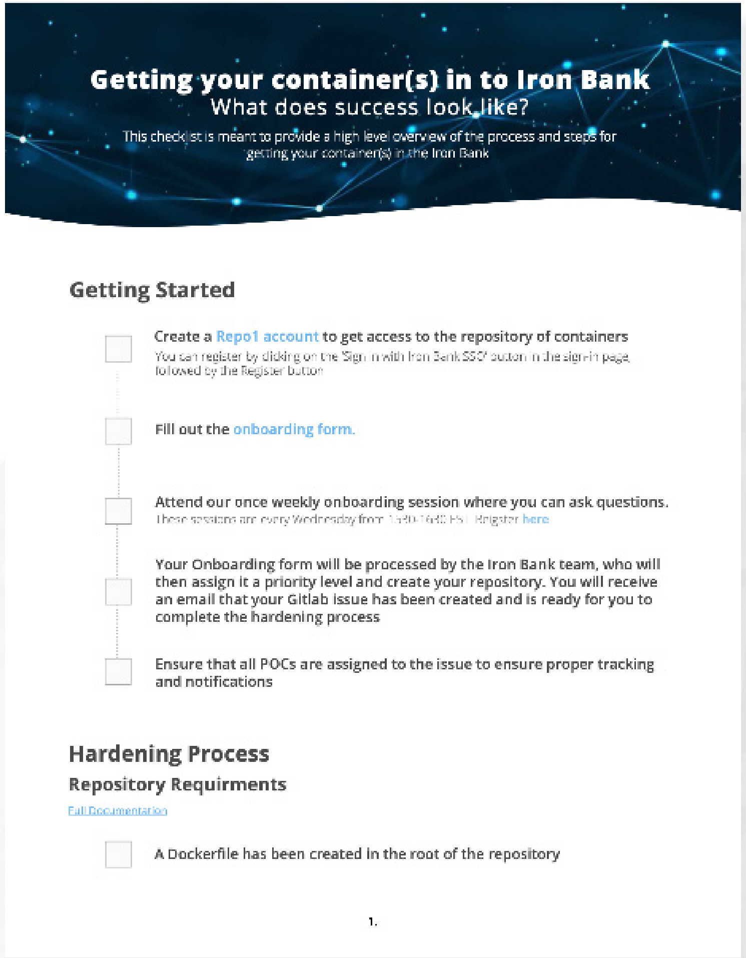
Our Methodology

Containers must follow a rigorous set of processes and requirements in order to receive an approval

Technical requirements and details can be found in this Contributor Onboarding Guide. However, at a high level, applications must follow the following requirements:

- Rebasing the container onto an approved base image (Red Hat UBI, distroless, etc)
- Internet disconnected build processes
- The application and all containers must be supported by a vendor, open source community, or government entity
- You must be working with the latest of the release series for your dependencies and application
- Timely justifications of all findings from the following scanners:
  - OpenSCAP: DISA STIG compliance
  - Twistlock: CVE identification
  - Anchore: CVE and DoD compliance identification
- Continuous monitoring (currently every 12 hours) and timely submission of justifications for any new findings
- Submission of any new application update(s) no later than the day of public release

Onboarding Checklist



Getting your container(s) in to Iron Bank

What does success look like?

This checklist is meant to provide a high level overview of the process and steps for getting your container(s) in the Iron Bank

Getting Started

□ Create a Repo1 account to get access to the repository of containers
You can register by clicking on the 'Sign in with Iron Bank SSO' button in the sign-in page, followed by the Register button

□ Fill out the onboarding form.

□ Attend our once weekly onboarding session where you can ask questions.
These sessions are every Wednesday from 1530-1630 EST. Register here

□ Your Onboarding form will be processed by the Iron Bank team, who will then assign it a priority level and create your repository. You will receive an email that your Gitlab issue has been created and is ready for you to complete the hardening process

□ Ensure that all POCs are assigned to the issue to ensure proper tracking and notifications

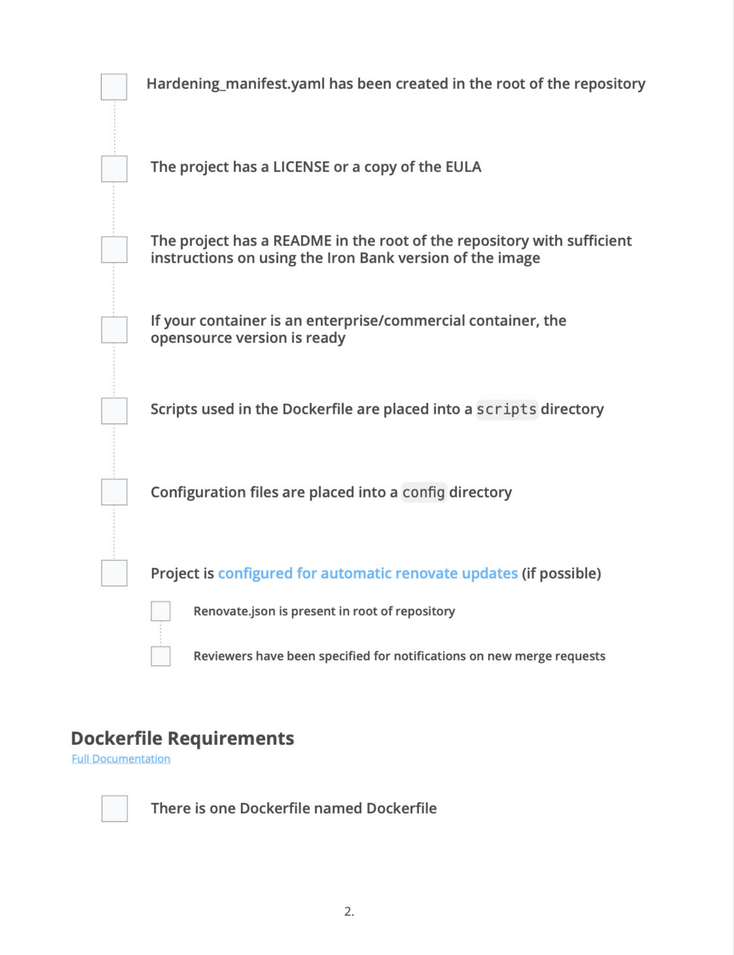
Hardening Process

Repository Requirments

Full Documentation

□ A Dockerfile has been created in the root of the repository

1.



□ Hardening_manifest.yaml has been created in the root of the repository

□ The project has a LICENSE or a copy of the EULA

□ The project has a README in the root of the repository with sufficient instructions on using the Iron Bank version of the image

□ If your container is an enterprise/commercial container, the opensource version is ready

□ Scripts used in the Dockerfile are placed into a `scripts` directory

□ Configuration files are placed into a `config` directory

□ Project is configured for automatic renovate updates (if possible)

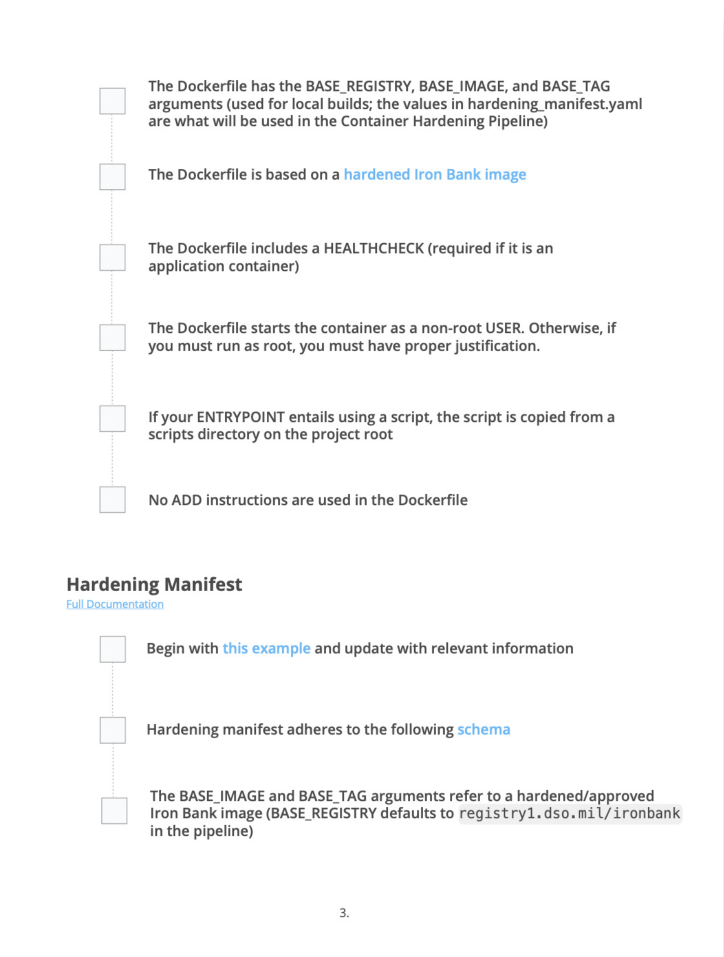
- □ Renovate.json is present in root of repository
- □ Reviewers have been specified for notifications on new merge requests

Dockerfile Requirements

Full Documentation

□ There is one Dockerfile named Dockerfile

2.



□ The Dockerfile has the BASE_REGISTRY, BASE_IMAGE, and BASE_TAG arguments (used for local builds; the values in hardening_manifest.yaml are what will be used in the Container Hardening Pipeline)

□ The Dockerfile is based on a hardened Iron Bank image

□ The Dockerfile includes a HEALTHCHECK (required if it is an application container)

□ The Dockerfile starts the container as a non-root USER. Otherwise, if you must run as root, you must have proper justification.

□ If your ENTRYPOINT entails using a script, the script is copied from a scripts directory on the project root

□ No ADD instructions are used in the Dockerfile

Hardening Manifest

Full Documentation

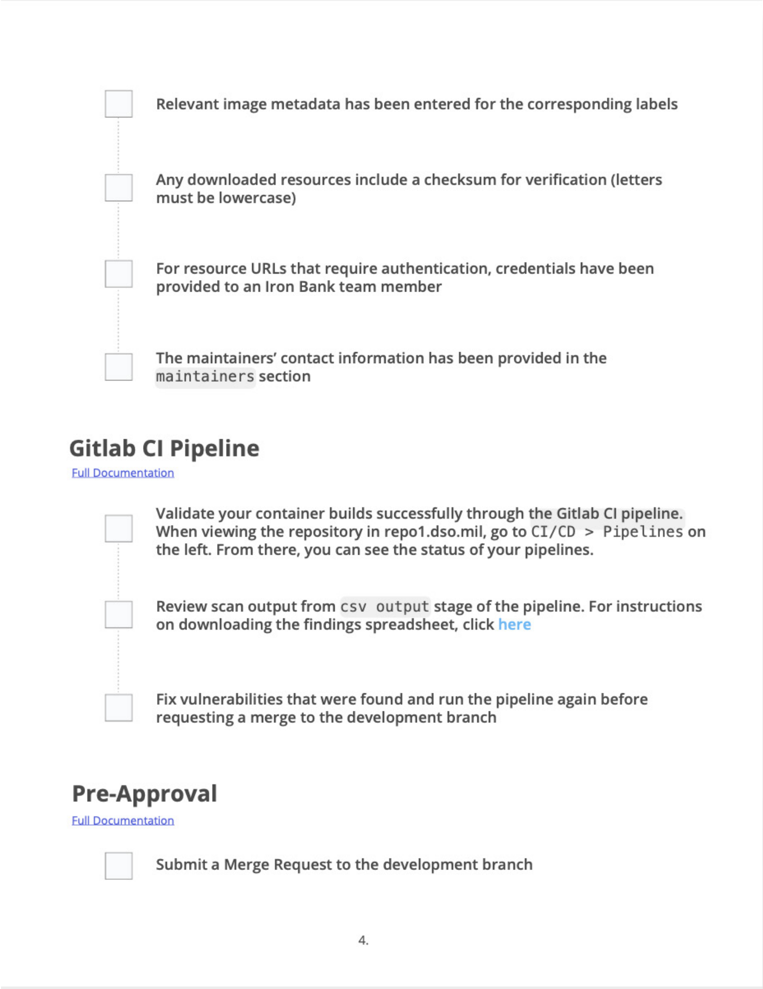
□ Begin with this example and update with relevant information

□ Hardening manifest adheres to the following schema

□ The BASE_IMAGE and BASE_TAG arguments refer to a hardened/approved Iron Bank image (BASE_REGISTRY defaults to `registry1.dso.mil/ironbank` in the pipeline)

3.

Onboarding Checklist



□ Relevant image metadata has been entered for the corresponding labels

□ Any downloaded resources include a checksum for verification (letters must be lowercase)

□ For resource URLs that require authentication, credentials have been provided to an Iron Bank team member

□ The maintainers' contact information has been provided in the `maintainers` section

Gitlab CI Pipeline

Full Documentation

□ Validate your container builds successfully through the Gitlab CI pipeline. When viewing the repository in repo1.dso.mil, go to `CI/CD > Pipelines` on the left. From there, you can see the status of your pipelines.

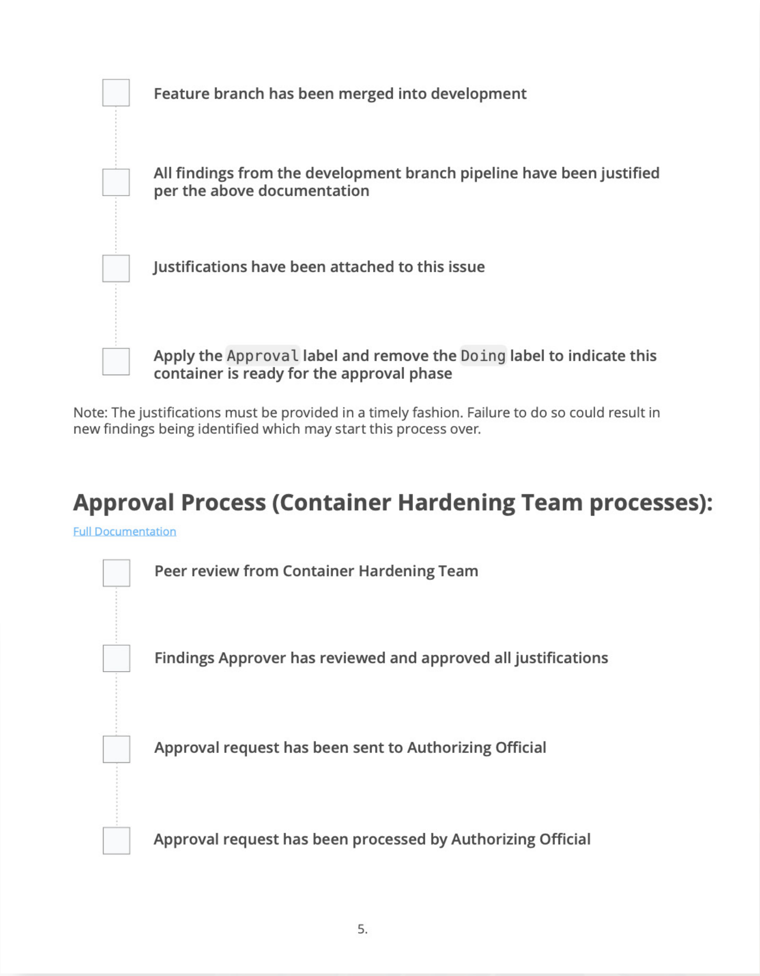
□ Review scan output from `csv output` stage of the pipeline. For instructions on downloading the findings spreadsheet, click here

□ Fix vulnerabilities that were found and run the pipeline again before requesting a merge to the development branch

Pre-Approval

Full Documentation

□ Submit a Merge Request to the development branch



□ Feature branch has been merged into development

□ All findings from the development branch pipeline have been justified per the above documentation

□ Justifications have been attached to this issue

□ Apply the `Approval` label and remove the `Doing` label to indicate this container is ready for the approval phase

Note: The justifications must be provided in a timely fashion. Failure to do so could result in new findings being identified which may start this process over.

Approval Process (Container Hardening Team processes):

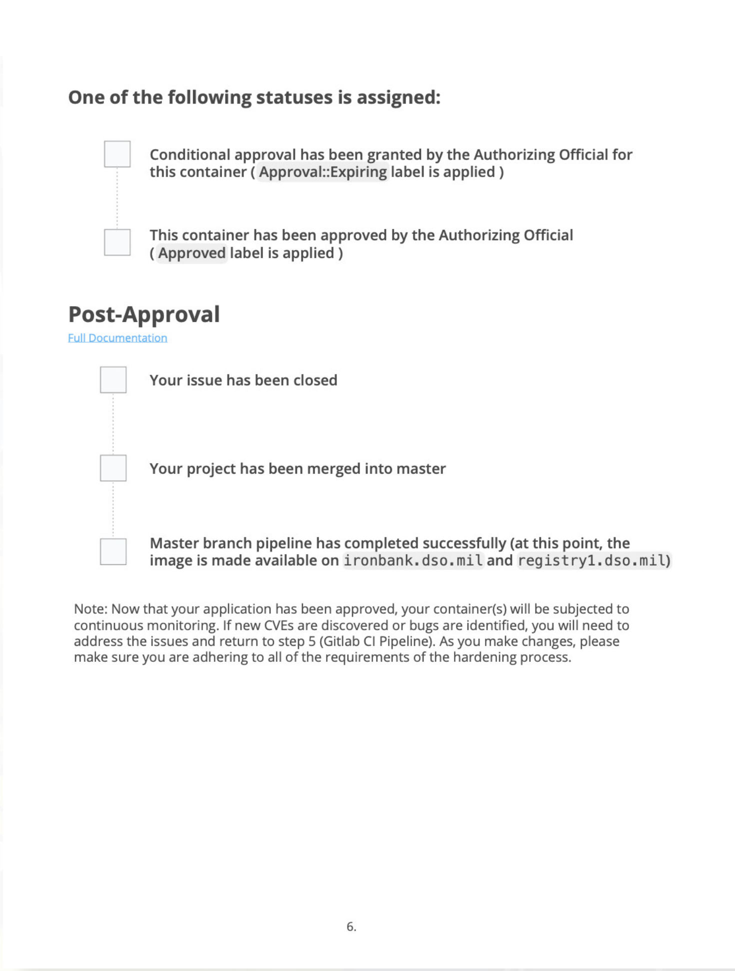
Full Documentation

□ Peer review from Container Hardening Team

□ Findings Approver has reviewed and approved all justifications

□ Approval request has been sent to Authorizing Official

□ Approval request has been processed by Authorizing Official



One of the following statuses is assigned:

□ Conditional approval has been granted by the Authorizing Official for this container (Approval::Expiring label is applied)

□ This container has been approved by the Authorizing Official (Approved label is applied)

Post-Approval

Full Documentation

□ Your issue has been closed

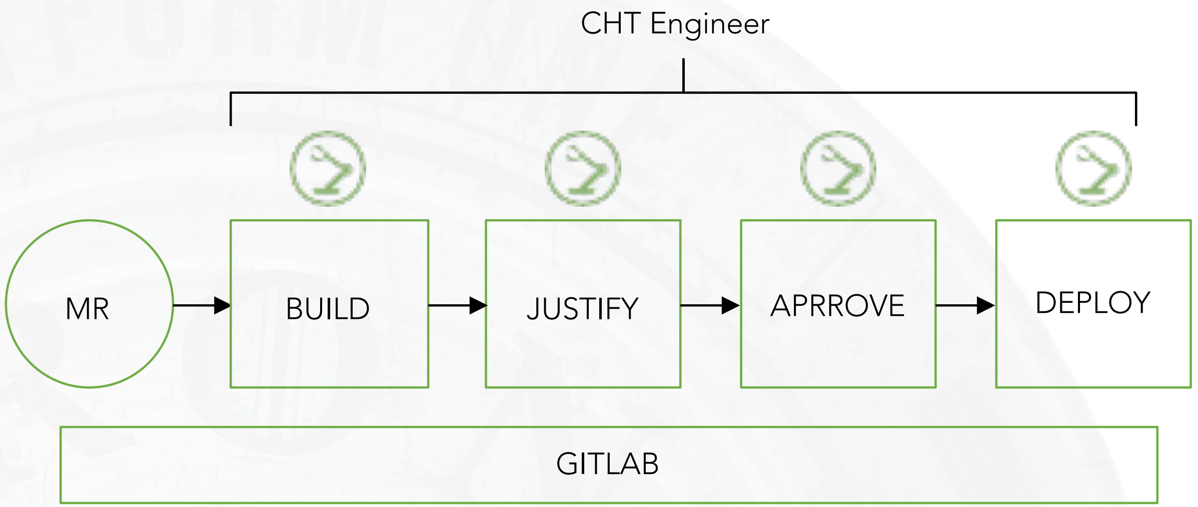
□ Your project has been merged into master

□ Master branch pipeline has completed successfully (at this point, the image is made available on `ironbank.dso.mil` and `registry1.dso.mil`)

Note: Now that your application has been approved, your container(s) will be subjected to continuous monitoring. If new CVEs are discovered or bugs are identified, you will need to address the issues and return to step 5 (Gitlab CI Pipeline). As you make changes, please make sure you are adhering to all of the requirements of the hardening process.

Merge Requests

The onboarding form described previously serves as the method to request hardening, in Gitlab, your issue is the way to track the status of the work performed, however, the hardening effort is not invoked until a merge request is made (see diagram below).



Tracking Work Status

In order to track the status of your request, we have created labels for easy tracking of your project through the Iron Bank process.

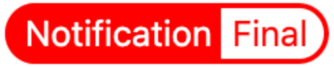
Where do I check on the status of my container?

You should have access to this https://repo1.dsop.io/dsop and be checking on the status of your containers here.

How do you communicate the current status of the project?

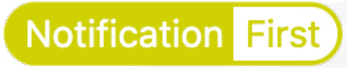
Please use the comment box's on each of the issues, this allows for transparent tracking. Do not just email your POC directly. What happens in the pipeline and how to tell where you are at? Use these labels to learn more about the flow and how to tell the status of your project. https://repo1.dsop.io/groups/dsop/-/labels

Tracking Work Status Labels



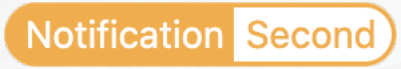
Notification Final

Final notification after 42 days of inactivity, the issue is being moved to Iron Bank Leadership to adjudicate why no work is happening.



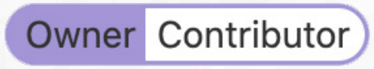
Notification First

An Automated label to notify of inactivity - applied after 14 days of no update to the issue.



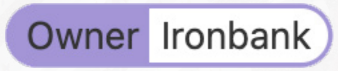
Notification Second

An Automated label to notify of inactivity - applied after 28 days of no update to the issue.



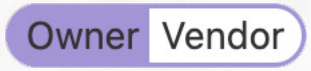
Owner Contributor

All work is owned by an external contributor, an external entity who is a partner with Platform One is managing the containerization and updates to this product.



Owner Ironbank

All work is owned by members of the Container Hardening Team within Iron Bank.



Owner Vendor

A Vendor is managing the containerization and updates to this product. All work is owned by the vendor with the exception of the approval process.

Understanding Labels

Approval	A Container is ready to go through the approval process and at this point the work is being handed off to the Iron Bank team to manage the approval.
Approval Expiring	Containers whose approval is expiring soon
Approval Local Review	The container is going through Local Review prior to final submission (we are aiming for an average of 3-5 business days) for this stage.
Approval Local Security	The container is going through Local Security Review prior to a Local Review for approval (we are aiming for an average of 3-5 business days) for this stage.
Approval Official Review	The container is going through an Official Review from the authorizing official and we are awaiting the final approval and or comments.
Approved	Container has been officially approved
Awaiting Response	Awaiting response from contributor

Understanding Labels

Blocked	There is something blocking the container
Bug	Problems with existing features/functionality
Container Archive	Archive an application
Container Initial	Initial hardening of container: This is the first time a container is going through the Iron Bank pipeline.
Container Justifications	Containers in the justification process
Container New Findings	Containers that have new findings based on continuous monitoring, that need to be addressed before being approved again.
Container Update	Containers that are being updated to a new version

Understanding Priority Labels

PRIORITY 0

Tickets requested to be prioritized by the P1 Leadership team

PRIORITY 1

Platform One Core Container - Impacts BB + PB + IB

PRIORITY 2

Core items for Iron Bank Pipelines (defined by Josh and Clarissa)

PRIORITY 3

Core Package Items for Big Bang Pipelines (defined by Toby Oswald)

PRIORITY 4

This priority is used for any tools, products or items that are used as part of the PlatformOne core infrastructure (Party Bus, CNAP, Cyber, Customer Success)

PRIORITY 5

This priority is used for paying customers of Platform One. Money must be already sent to Platform One for this priority to be applied. Tier ONE on the True Up initiative = A customer paying > $4M

PRIORITY 6

Tier TWO on the True Up initiative = A customer paying between < $3.9M > $500K

Understanding Priority Labels

PRIORITY 7 — Tier THREE on the True Up initiative = A customer paying < $499K and > $80K

PRIORITY 8 — Open Source containers that are used by the community and supported by Iron Bank for the utility of Platform One Services

PRIORITY 9 — This priority is used for projects where there is a specific DoD/Govt customer identified and the vendor needs to get through Iron Bank before the gov customer can use the service. Potential Platform One customers who are working on payment or are interested in paying Platform One.

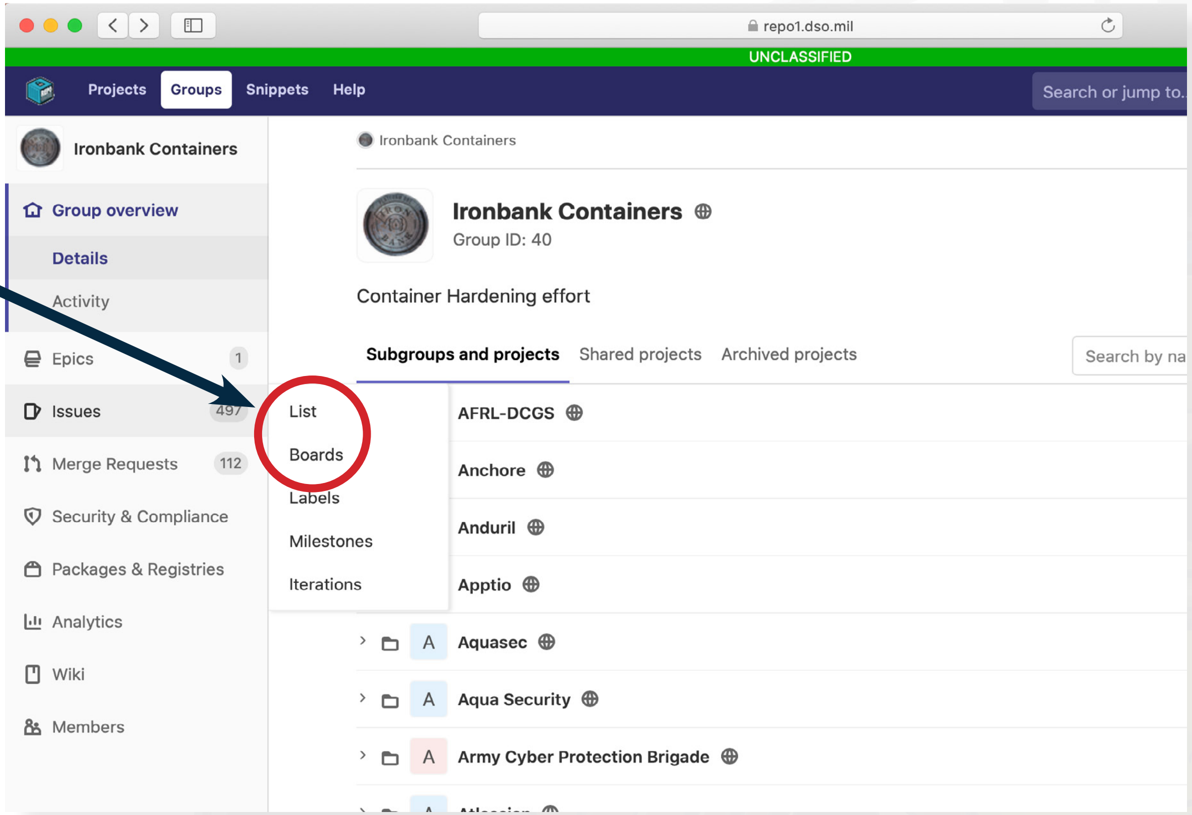
PRIORITY 10 — This is for vendor’s containers who do not have a DoD/Govt customer identified but want to get their containers approved for use on Iron Bank.

PRIORITY 11 — This is for open source containers that do not have a DoD/Govt customer identified and no defined user base.

Status Tracking Example

Repo1.dso.mil > Single Sign On > Iron Bank Git Repository

List and Board Options!



repo1.dso.mil

UNCLASSIFIED

Ironbank Containers

Ironbank Containers
Group ID: 40

Container Hardening effort

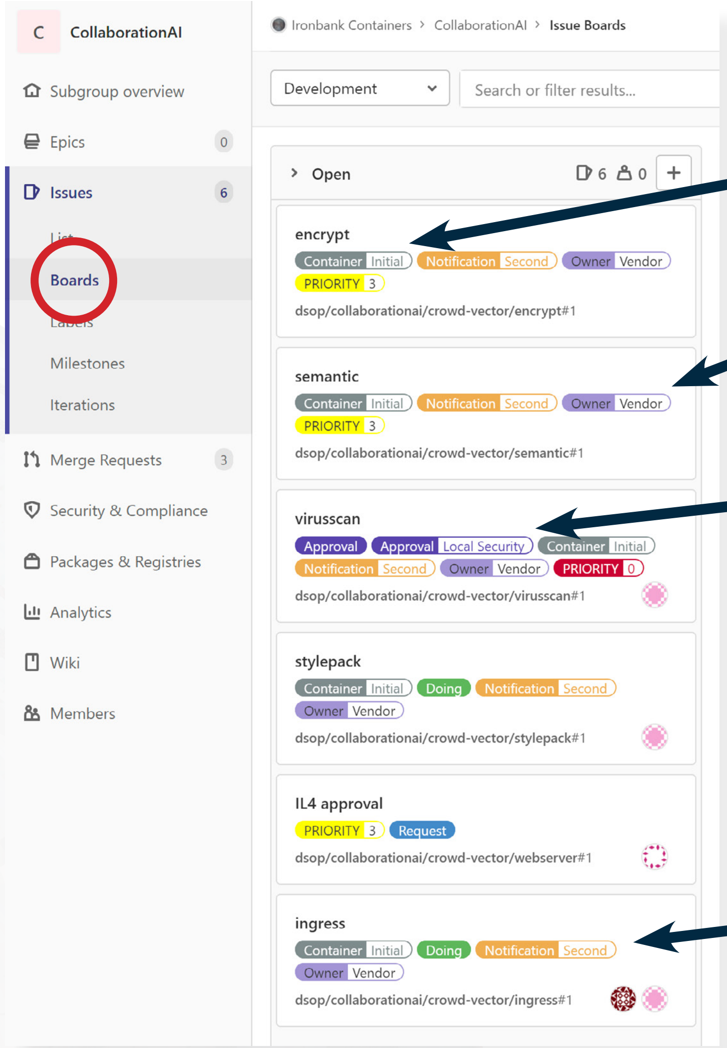
Subgroups and projects | Shared projects | Archived projects | Search by na

- AFRL-DCGS
- Anchore
- Anduril
- Apptio
- A Aquasec
- A Aqua Security
- A Army Cyber Protection Brigade

Status Tracking Example

In order to track the status of your request, we have created labels for easy tracking of your project through the Iron Bank process.

Here in the board view, you can search, see the container, initial tag, see an issue in approval, and see that work is still being done.



C CollaborationAI

Subgroup overview

Epics 0

Issues 6

List

Boards

Labels

Milestones

Iterations

Merge Requests 3

Security & Compliance

Packages & Registries

Analytics

Wiki

Members

Ironbank Containers › CollaborationAI › Issue Boards

Development

Search or filter results...

Open 6 0 +

encrypt

Container Initial | Notification Second | Owner Vendor | PRIORITY 3

dsop/collaborationai/crowd-vector/encrypt#1

semantic

Container Initial | Notification Second | Owner Vendor | PRIORITY 3

dsop/collaborationai/crowd-vector/semantic#1

virusscan

Approval | Approval Local Security | Container Initial | Notification Second | Owner Vendor | PRIORITY 0

dsop/collaborationai/crowd-vector/virusscan#1

stylepack

Container Initial | Doing | Notification Second | Owner Vendor

dsop/collaborationai/crowd-vector/stylepack#1

IL4 approval

PRIORITY 3 | Request

dsop/collaborationai/crowd-vector/webserver#1

ingress

Container Initial | Doing | Notification Second | Owner Vendor

dsop/collaborationai/crowd-vector/ingress#1

First time that a container is going through

Who the owner is - Vendors must do all their own hardening

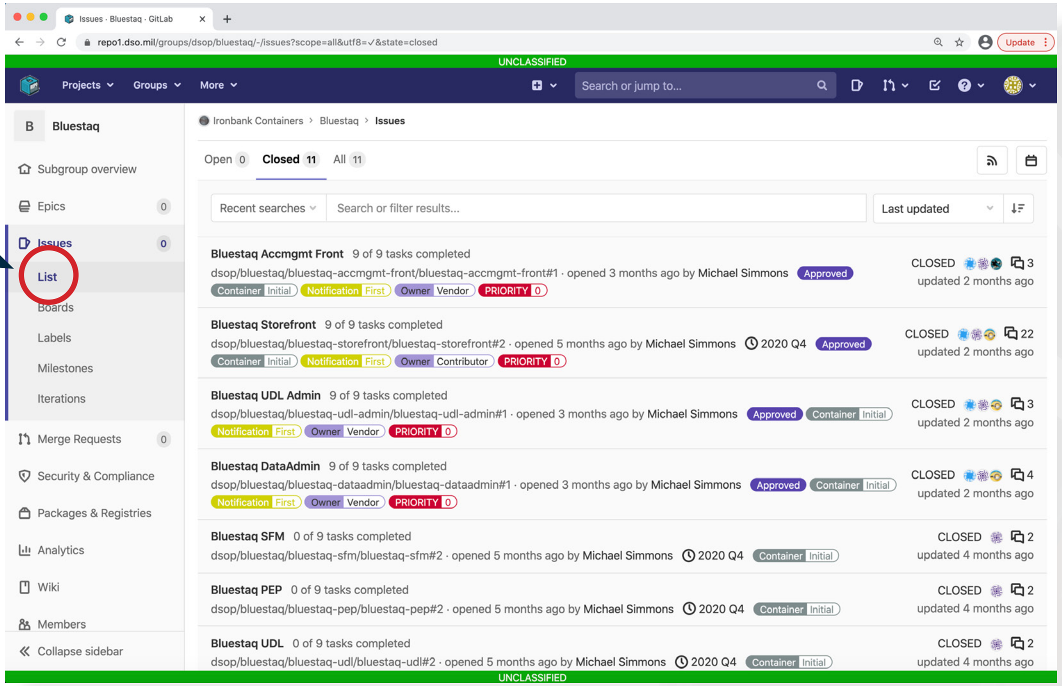
This container is going through the approval process and is with local security!

Notification tag's show up here as well if progress is not being communicated.

Status Tracking Example

Repo1.dso.mil > Single Sign On > Iron Bank Git Repository

List View of a particular set of containers. Notice the labels, they tell you where things are in the process!



Bluestaq Accmgmt Front 9 of 9 tasks completed
dsop/bluestaq/bluestaq-accmgmt-front/bluestaq-accmgmt-front#1 · opened 3 months ago by Michael Simmons Approved
Container Initial · Notification First · Owner Vendor · PRIORITY 0
CLOSED 3 · updated 2 months ago

Bluestaq Storefront 9 of 9 tasks completed
dsop/bluestaq/bluestaq-storefront/bluestaq-storefront#2 · opened 5 months ago by Michael Simmons 2020 Q4 Approved
Container Initial · Notification First · Owner Contributor · PRIORITY 0
CLOSED 22 · updated 2 months ago

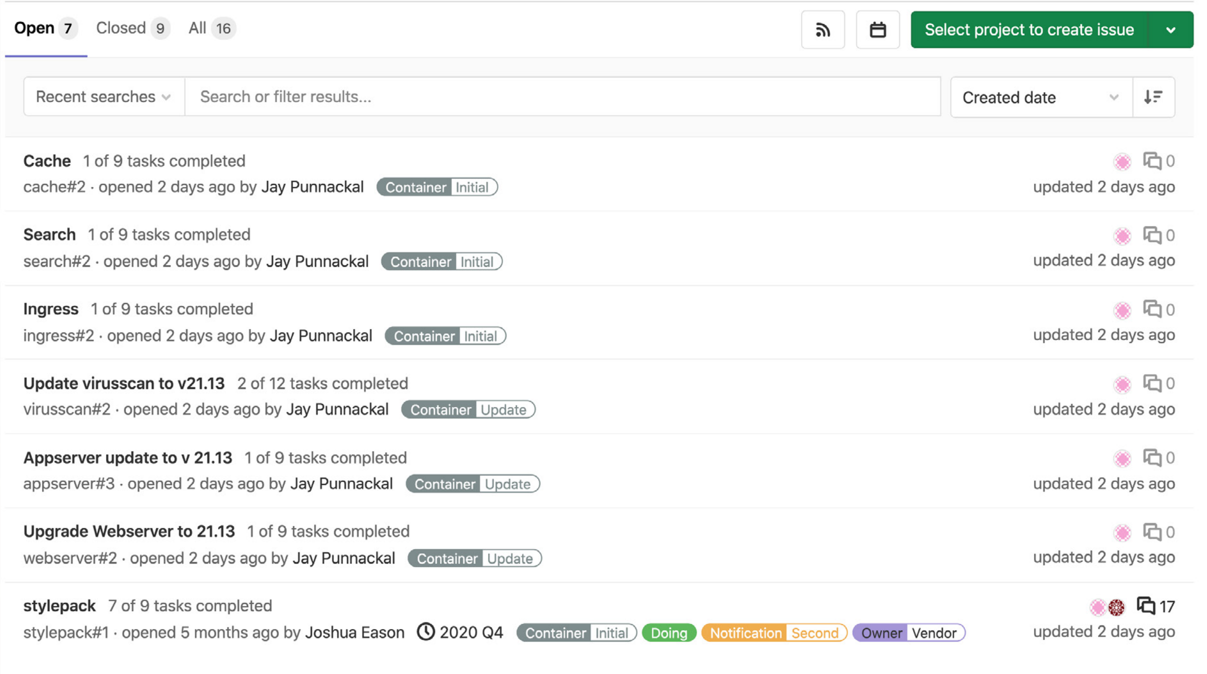
Bluestaq UDL Admin 9 of 9 tasks completed
dsop/bluestaq/bluestaq-udl-admin/bluestaq-udl-admin#1 · opened 3 months ago by Michael Simmons Approved · Container Initial
Notification First · Owner Vendor · PRIORITY 0
CLOSED 3 · updated 2 months ago

Bluestaq DataAdmin 9 of 9 tasks completed
dsop/bluestaq/bluestaq-dataadmin/bluestaq-dataadmin#1 · opened 3 months ago by Michael Simmons Approved · Container Initial
Notification First · Owner Vendor · PRIORITY 0
CLOSED 4 · updated 2 months ago

Bluestaq SFM 0 of 9 tasks completed
dsop/bluestaq/bluestaq-sfm/bluestaq-sfm#2 · opened 5 months ago by Michael Simmons 2020 Q4 Container Initial
CLOSED 2 · updated 4 months ago

Bluestaq PEP 0 of 9 tasks completed
dsop/bluestaq/bluestaq-pep/bluestaq-pep#2 · opened 5 months ago by Michael Simmons 2020 Q4 Container Initial
CLOSED 2 · updated 4 months ago

Bluestaq UDL 0 of 9 tasks completed
dsop/bluestaq/bluestaq-udl/bluestaq-udl#2 · opened 5 months ago by Michael Simmons 2020 Q4 Container Initial
CLOSED 2 · updated 4 months ago



Cache 1 of 9 tasks completed
cache#2 · opened 2 days ago by Jay Punnackal Container Initial
0 · updated 2 days ago

Search 1 of 9 tasks completed
search#2 · opened 2 days ago by Jay Punnackal Container Initial
0 · updated 2 days ago

Ingress 1 of 9 tasks completed
ingress#2 · opened 2 days ago by Jay Punnackal Container Initial
0 · updated 2 days ago

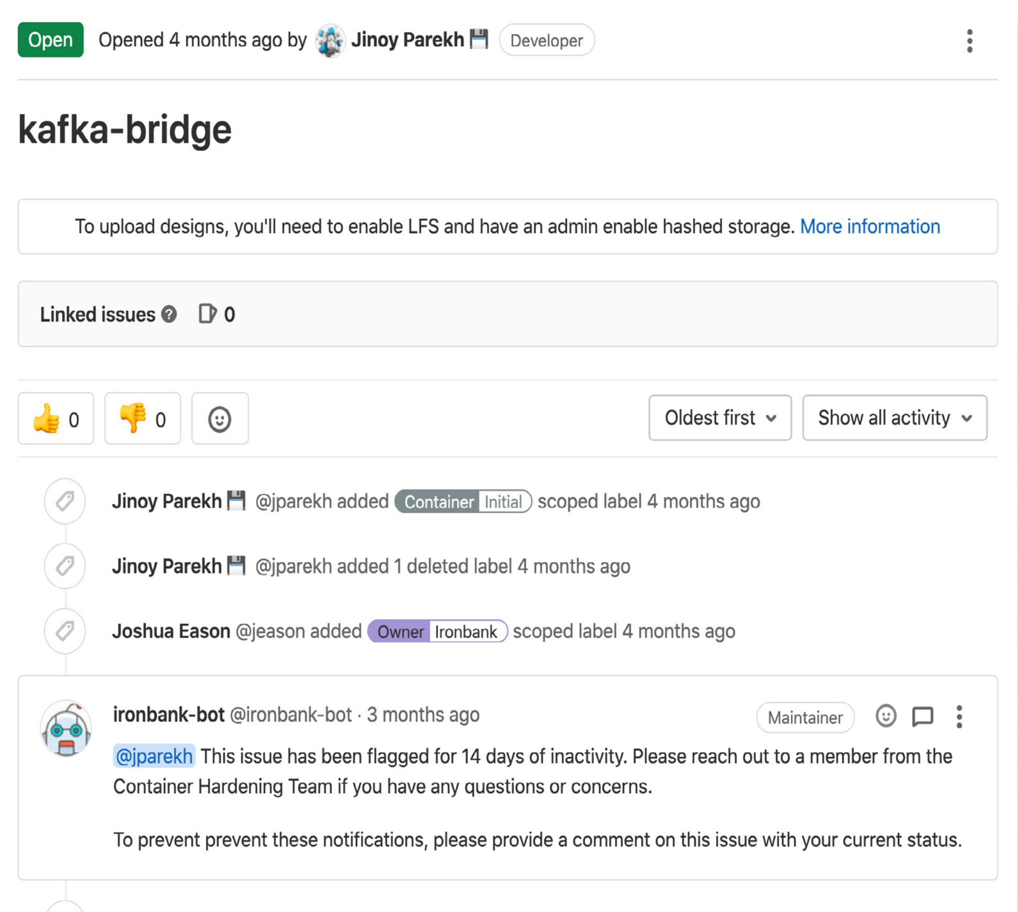
Update virusscan to v21.13 2 of 12 tasks completed
virusscan#2 · opened 2 days ago by Jay Punnackal Container Update
0 · updated 2 days ago

Appserver update to v 21.13 1 of 9 tasks completed
appserver#3 · opened 2 days ago by Jay Punnackal Container Update
0 · updated 2 days ago

Upgrade Webserver to 21.13 1 of 9 tasks completed
webserver#2 · opened 2 days ago by Jay Punnackal Container Update
0 · updated 2 days ago

stylepack 7 of 9 tasks completed
stylepack#1 · opened 5 months ago by Joshua Eason 2020 Q4 Container Initial · Doing · Notification Second · Owner Vendor
17 · updated 2 days ago

Status Tracking Example



Open Opened 4 months ago by Jinoy Parekh 💾 Developer

kafka-bridge

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Linked issues ? 0

👍 0 👎 0 ☺ Oldest first ⌄ Show all activity ⌄

Jinoy Parekh 💾 @jparekh added Container Initial scoped label 4 months ago

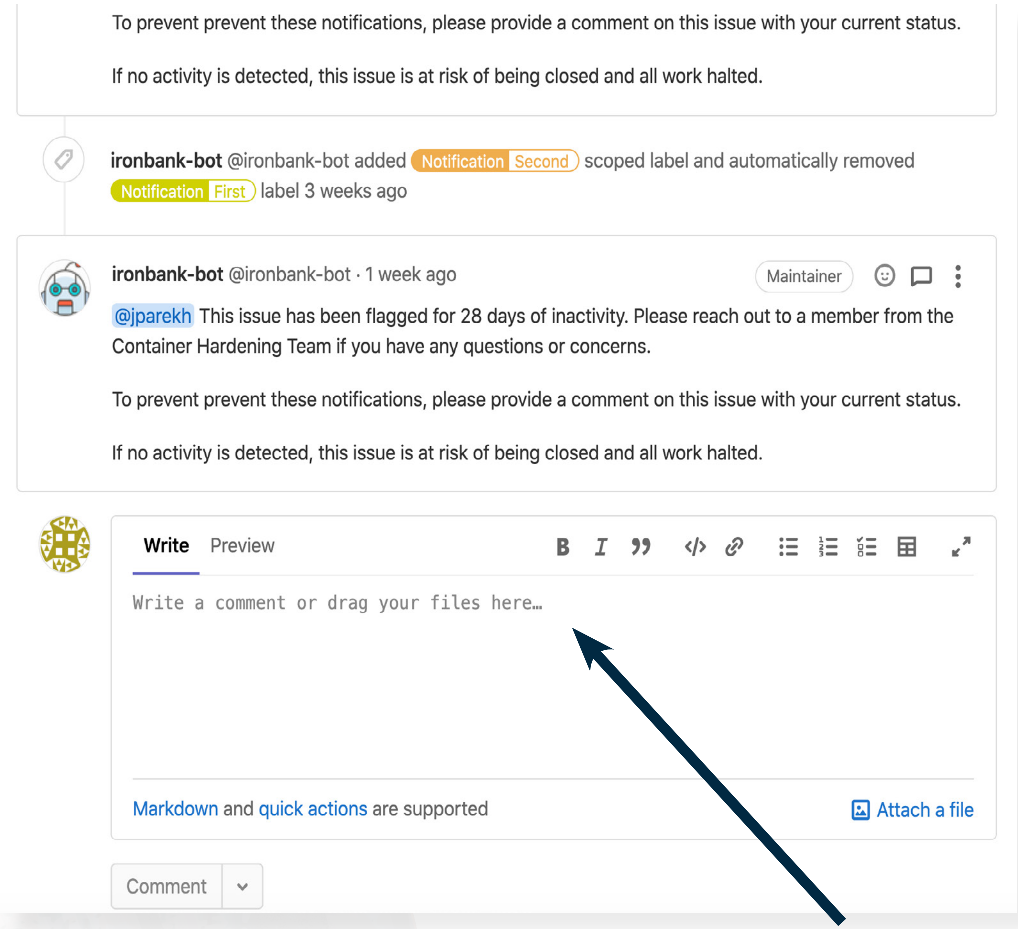
Jinoy Parekh 💾 @jparekh added 1 deleted label 4 months ago

Joshua Eason @jeason added Owner Ironbank scoped label 4 months ago

ironbank-bot @ironbank-bot · 3 months ago Maintainer

@jparekh This issue has been flagged for 14 days of inactivity. Please reach out to a member from the Container Hardening Team if you have any questions or concerns.

To prevent prevent these notifications, please provide a comment on this issue with your current status.



To prevent prevent these notifications, please provide a comment on this issue with your current status.

If no activity is detected, this issue is at risk of being closed and all work halted.

ironbank-bot @ironbank-bot added Notification Second scoped label and automatically removed Notification First label 3 weeks ago

ironbank-bot @ironbank-bot · 1 week ago Maintainer

@jparekh This issue has been flagged for 28 days of inactivity. Please reach out to a member from the Container Hardening Team if you have any questions or concerns.

To prevent prevent these notifications, please provide a comment on this issue with your current status.

If no activity is detected, this issue is at risk of being closed and all work halted.

Write Preview

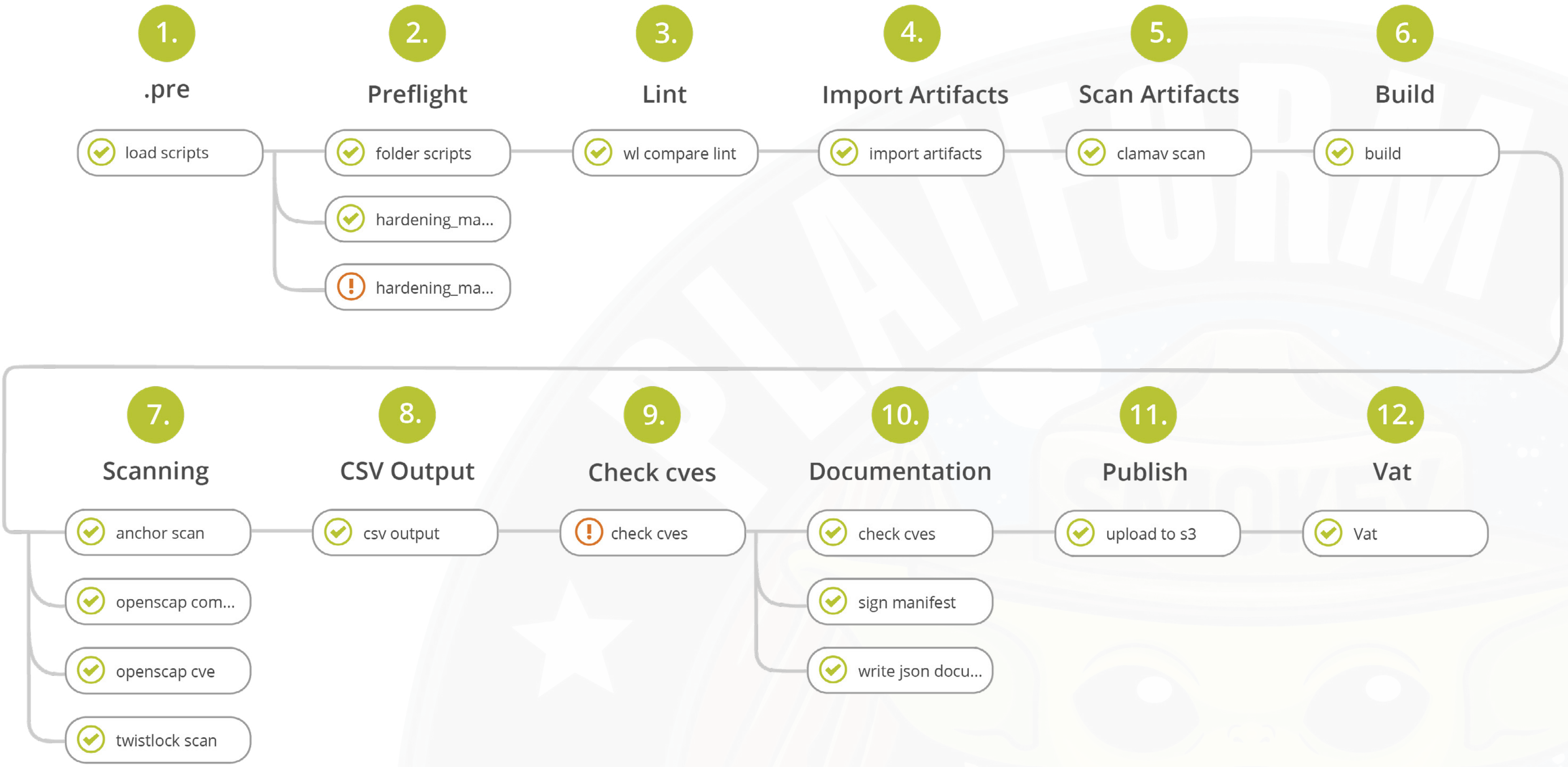
Write a comment or drag your files here…

Markdown and quick actions are supported Attach a file

Comment ⌄

Write comments here

The Hardening Pipeline



1. .pre
- ✓ load scripts

2. Preflight
- ✓ folder scripts
- ✓ hardening_ma...
- ! hardening_ma...

3. Lint
- ✓ wl compare lint

4. Import Artifacts
- ✓ import artifacts

5. Scan Artifacts
- ✓ clamav scan

6. Build
- ✓ build

7. Scanning
- ✓ anchor scan
- ✓ openscap com...
- ✓ openscap cve
- ✓ twistlock scan

8. CSV Output
- ✓ csv output

9. Check cves
- ! check cves

10. Documentation
- ✓ check cves
- ✓ sign manifest
- ✓ write json docu...

11. Publish
- ✓ upload to s3

12. Vat
- ✓ Vat

Final Reminders

Good things to remember!

- You must comment on your issue if you need any help, or come to the Get Unstuck Sessions – no email
- Your repositories will be public
- You MUST respond to every finding
- Do not change the priority labels. We will figure it out.

Documentation

- **Contributor Onboarding**
  https://repo1.dso.mil/dsop/dccscr/-/tree/master
- **Office of the Chief Software Officer**
  https://software.af.mil/
- **DSOP Services (DoD Enterprise DevSecOps)**
  https://software.af.mil/dsop/services/
- **DSOP Architecture at a Glance**
  https://software.af.mil/dsop/architecture/
- **Frequently Asked Questions (FAQ)**
  https://software.af.mil/dsop/frequently-asked-questions-faq/
- **DoD Centralized Artifacts Repository - DCAR**
  https://ironbank.dso.mil/ironbank/repomap
- **DoD Repo One Code Repository**
  https://repo1.dsop.io/users/sign_in

Q & A

Feel free to ask questions!